

A SUFFICIENT CONDITION FOR A NUMBER TO BE THE ORDER OF A NONSINGULAR DERIVATION OF A LIE ALGEBRA

S. MATTAREI

ABSTRACT. A study of the set \mathcal{N}_p of positive integers which occur as orders of nonsingular derivations of finite-dimensional non-nilpotent Lie algebras of characteristic $p > 0$ was initiated by Shalev and continued by the present author. The main goal of this paper is to produce more elements of \mathcal{N}_p . Our main result shows that any divisor n of $q - 1$, where q is a power of p , such that $n \geq (p - 1)^{1/p}(q - 1)^{1 - 1/(2p)}$, necessarily belongs to \mathcal{N}_p . This extends its special case for $p = 2$ which was proved in a previous paper by a different method.

1. INTRODUCTION

Finite-dimensional Lie algebras which admit a nonsingular (that is, injective) derivation play a role in various investigations. Some of those are discussed in the Introduction of [Mat], of which this paper is a continuation. We briefly recall here only the essential facts relevant to our present study and refer to [Mat] and its predecessor [Mat02] for more details.

According to a classical result of Jacobson [Jac79, p. 54], in characteristic zero only nilpotent Lie algebras can have nonsingular derivations. In positive characteristic, where even certain simple Lie algebras can admit nonsingular derivations, the same argument would be inconclusive, but still imposes a strong restriction of the eigenvalues (assumed in the ground field) of a nonsingular derivation of a non-nilpotent Lie algebra. In particular, if the derivation has finite order n , as is relevant to various studies, this restriction entails an interesting necessary condition on n , noted by Shalev in [Sha99]. The condition was shown to be sufficient as well in [Mat02]. We recall both implications as Theorem 2.1 in the next section.

More generally, in his paper [Sha99] Shalev suggested and initiated a study of the set \mathcal{N}_p of positive integers which occur as the orders of nonsingular derivations of finite-dimensional non-nilpotent Lie algebras of prime characteristic p . Theorem 2.1 translates this problem into one entirely formulated in terms of finite fields. Therefore, no Lie algebra argument will be used in this paper. It is easy to see that \mathcal{N}_p is closed with respect to taking multiples, and that a positive integer n belongs to \mathcal{N}_p if and only if its p' -part does. Thus, one may restrict one's attention to numbers in \mathcal{N}_p which are prime to p . Even after this restriction, rather trivial elements of \mathcal{N}_p are those of the form $p^k - 1$ for some $k \geq 2$, as will be clear from Theorem 2.1. We will conveniently call *nontrivial* elements of \mathcal{N}_p those numbers in \mathcal{N}_p which are prime to p and are not multiples of any $p^k - 1$ with $k \geq 2$. Shalev proved in [Sha99] that no nontrivial element of \mathcal{N}_p is smaller than p^2 . This was extended in [Mat02, Lemma 3.2], to conclude that no nontrivial element of \mathcal{N}_p is smaller than p^3 , except for $(3^3 - 1)/2 = 13$ when $p = 3$.

Date: February 1, 2008.

2000 Mathematics Subject Classification. Primary 17B50; secondary 17B40, 12C15, 20C15.

Key words and phrases. Modular Lie algebras, nonsingular derivations, equations over finite fields.

(This exception has an analogue for all odd primes, see the next paragraph.) In fact, we do not know of any nontrivial element of \mathcal{N}_p which is smaller than p^4 , except for 13 when $p = 3$.

In the opposite direction, one nontrivial element of \mathcal{N}_p is $(p^p - 1)/(p - 1)$, for odd p , as noted by Shalev in [Sha99, Example 2.6]. For $p = 2$ many numbers in \mathcal{N}_2 were disclosed in [Mat]. Apart from the special series of numbers of the form $n = (2^{3s} - 1)/(2^s - 1)$, of which the case $s = 3$ (whence $n = 73$) was already noted by Shalev in [Sha99], we proved a result guaranteeing that all divisors of $q - 1$, where q is a power of 2, which are large enough in an appropriate sense belong to \mathcal{N}_2 . Explicitly, a sufficient condition for a divisor n of $q - 1$ to belong to \mathcal{N}_2 was found to be that $n \geq (q - 1)^{3/4}$. However, the arguments used in [Mat], based on the character theory of a certain group, were limited to the case of the prime 2.

In this paper we extend that result to an arbitrary prime p . We prove in Corollary 2.5 that a divisor n of $q - 1$, where q is a power of p , belongs to \mathcal{N}_p provided it satisfies the inequality $n \geq (p - 1)^{1/p}(q - 1)^{1 - 1/(2p)}$. This is a weaker and simplified form of a more precise sufficient condition for a certain system of equations having solutions over the finite field \mathbb{F}_q . We prove that in Section 4 by means of standard character sum estimates. We sketch a less elementary but shorter proof in Remark 4.3.

In Section 3 we have collected several remarks on the set \mathcal{N}_p . In particular, we discuss some consequences of our main result, present the outcome of some computer calculations, discuss the density of the set of integers \mathcal{N}_p (following a suggestion of a referee) and a notion of relative size of its elements.

2. LARGE DIVISORS OF $q - 1$ BELONG TO \mathcal{N}_p

As mentioned in the Introduction, \mathcal{N}_p denotes the set of positive integers n for which there exists finite-dimensional non-nilpotent Lie algebra L , over a field of characteristic p , which admits a nonsingular derivation of order n . We recall from [Mat02, Corollary 2.3] the essential part of a characterization of the elements of \mathcal{N}_p which are prime to p .

Theorem 2.1. *A positive integer n prime to p belongs to \mathcal{N}_p if and only if there exists an element ξ of the algebraic closure $\bar{\mathbb{F}}_p$ of \mathbb{F}_p , such that $(\xi + \lambda)^n = 1$ for all $\lambda \in \mathbb{F}_p$.*

This condition is trivially satisfied by numbers n of the form $p^k - 1$ with $k \geq 2$, and hence those numbers belong to \mathcal{N}_p , together with their multiples. As anticipated in the Introduction, we call *trivial* those elements of \mathcal{N}_p , and *nontrivial* the others.

In general, for any n prime to p there is a power q of p such that n divides $q - 1$. For example, we may take $q = p^k$, where k is the multiplicative order of p modulo n . Then the condition $n \in \mathcal{N}_p$ is equivalent to the fact that there exists an element ξ of the finite field \mathbb{F}_q , such that $\xi, \xi + 1, \dots, \xi + p - 1$ are nonzero d th powers in \mathbb{F}_q , where $d = (q - 1)/n$. The following result provides an estimate for the number of such elements ξ , in a more general setting.

Theorem 2.2. *Let d be a divisor of $q - 1$ and let $0 < r \leq p$. Let M be the number of elements ξ of \mathbb{F}_q such that $\xi, \xi + 1, \dots, \xi + r - 1$ are nonzero d th powers in \mathbb{F}_q . Let M_0 be the number of elements ξ of \mathbb{F}_p such that $\xi, \xi + 1, \dots, \xi + r - 1$ include 0 and are d th powers in \mathbb{F}_q . Then*

$$\left| M + \frac{M_0 + 1}{d} - \frac{q + 1}{d^r} \right| \leq \left(r - 1 - \frac{r + 1}{d} + \frac{2}{d^r} \right) \sqrt{q}.$$

Since $0 \leq M_0 \leq r$ we deduce the bound

$$\left| M + \frac{r+1}{2d} - \frac{q+1}{d^r} \right| \leq \left(r - 1 - \frac{r+1}{d} + \frac{2}{d^r} \right) \sqrt{q} + \frac{r+1}{2d}.$$

which does not involve M_0 . Bounds of this type result from standard calculations with character sums, see [LN83, Exercises 5.65 and 5.66] or [Ste94, pp. 246-247]. Their simplest application is that, given d and r , for all primes p large enough there exists a sequence of r consecutive integers which are d th power residues modulo p . However, we are unable to quote from the literature a bound which is as sharp as that given in Theorem 2.2 (see the discussion in Remark 4.2), and hence we provide a proof in Section 4.

Here we need the special case of Theorem 2.2 where $r = p$. Then the lower bound for M reads

$$(2.1) \quad M \geq \frac{q+1}{d^p} - \frac{M_0+1}{d} - \left(p - 1 - \frac{p+1}{d} + \frac{2}{d^p} \right) \sqrt{q},$$

and M_0 can only be p or 0 , according as n is a multiple of $p-1$ or not. Then we know that n belongs to \mathcal{N}_p exactly when $M > 0$, where $d = (q-1)/n$. Thus, a sufficient condition for $n \in \mathcal{N}_p$ is that the right-hand side of inequality (2.1) be strictly positive. After a simple calculation this yields the following result.

Theorem 2.3. *Let q be a power of p and let n be a divisor of $q-1$. Then $n \in \mathcal{N}_p$ provided $d = (q-1)/n$ satisfies*

$$q - ((pd - p - d - 1)d^{p-1} + 2)\sqrt{q} - (p+1)d^{p-1} + 1 > 0.$$

If n is not a multiple of $(p-1)$, then the slightly weaker condition

$$q - ((pd - p - d - 1)d^{p-1} + 2)\sqrt{q} - d^{p-1} + 1 > 0$$

suffices.

Remark 2.4. For $p = 2$, where n is, necessarily, a multiple of $p-1$, the sufficient condition for $n \in \mathcal{N}_p$ given in Theorem 2.3 reads $q - (d-1)(d-2)\sqrt{q} - 3d + 1 > 0$. Once expressed in terms of $n = (q-1)/d$, the condition becomes $n^2 + 3(\sqrt{q}+1)n - \sqrt{q}(\sqrt{q}+1)^2 > 0$ or, equivalently, $n > (\sqrt{4\sqrt{q}+9} - 3)(\sqrt{q}+1)/2$. This is slightly weaker than the sufficient condition $n^4 > (q-n)^3$ given in [Mat, Theorem 3.1]. The reason is the following. As will be clear after section 4, especially Remark 4.2, when $p = 2$ the sufficient condition of Theorem 2.3 ultimately depends on Weil's bound $|N - d - q - 1| \leq (d-1)(d-2)\sqrt{q}$ for the number N of affine points of the Fermat curve $y_2^d - y_1^d = 1$ over \mathbb{F}_q . One can see that the proof of [Mat, Theorem 3.1] establishes and then uses a weaker bound than Weil's, with an error term close to $(d^2 - \frac{3}{2}d)\sqrt{q}$ rather than $(d^2 - 3d + 2)\sqrt{q}$.

A slightly weaker but more manageable form of the sufficient conditions given in Theorem 2.3 is the following.

Corollary 2.5. *Let q be a power of p and let n be a divisor of $q-1$ such that*

$$n \geq (p-1)^{1/p}(q-1)^{1-1/(2p)}.$$

Then $n \in \mathcal{N}_p$.

Note that the factor $(p-1)^{1/p}$ is always less than 1.32 and rapidly tends to 1 as p tends to infinity. When $p = 2$ the condition in Corollary 2.5 reads $n \geq (q-1)^{3/4}$, which is only slightly stronger than the condition $n^4 > (q-n)^3$ of [Mat, Theorem 3.1].

Proof. The former (and stronger) inequality in Theorem 2.3 can be equivalently written as

$$(\sqrt{q} - (p-1)d^p)(\sqrt{q} + (p+1)d^{p-1} - 2) + ((p-1)d^p - 1)((p+1)d^{p-1} - 2) > 1.$$

Temporarily viewing \sqrt{q} as a real variable, the inequality is satisfied when $\sqrt{q} = (p-1)d^p$, except when $p-1 = d = 1$. But in that case the conclusion of Corollary 2.5 holds trivially. Consequently, the inequality holds whenever $\sqrt{q} \geq (p-1)d^p$. In particular, it holds whenever $q-1 \geq (p-1)^2 d^{2p}$, which is equivalent with the stated hypothesis when written in terms of $n = (q-1)/d$. \square

Remark 2.6. Using the form of the inequality used in the proof of Corollary 2.5, one can easily see that the sufficient condition for $n \in \mathcal{N}_p$ given in Theorem 2.3 is asymptotic to the simpler one given in Corollary 2.5, in the sense that

$$\lim_{q \rightarrow \infty} (p-1)^{1/p} (q-1)^{1-1/(2p)} / f(q) = 1,$$

where $n > f(q)$ is an explicit form of the condition given in the former.

3. COMMENTS, CALCULATIONS, FURTHER QUESTIONS

3.1. Existence of proper divisors of $p^k - 1$ in \mathcal{N}_p . We discuss in which respect our main result produces nontrivial elements of \mathcal{N}_p . The following is an essentially equivalent formulation of Corollary 2.5 in terms of $d = (q-1)/n$ in place of n .

Corollary 3.1. *Let p be a prime and let d be a positive integer prime to p . If k is a positive multiple of the order of p modulo d then $(p^k - 1)/d \in \mathcal{N}_p$ provided $k \geq 2 + 2p \log d / \log p$.*

Proof. Setting $q = p^k$ and in terms of $d = (q-1)/n$, the sufficient condition of Corollary 2.5 becomes $p^k \geq (p-1)^2 d^{2p} + 1$, but the proof of Corollary 2.5 shows that the summand 1 can be discarded. Our present hypothesis $k \geq 2 + 2p \log d / \log p$ is only slightly stronger than that. \square

By taking $d = 2$ in Corollary 3.1 we see that, for every odd prime p and every integer $k \geq 2 + p \log 4 / \log p$, there is at least one proper divisor of $p^k - 1$ which belongs to \mathcal{N}_p , namely, $(p^k - 1)/2$. This statement is actually nontrivial only when k is prime, because otherwise $p^k - 1$ has proper divisors of the form $p^s - 1$ with $s > 1$, which are trivial elements of \mathcal{N}_p . Incidentally, note that the simplified condition of Corollary 3.1 (as well as that of Corollary 2.5) is notably weaker than the more precise Theorem 2.3 for small p and k . For example, Corollary 3.1 implies that $(3^k - 1)/2 \in \mathcal{N}_3$ for $k \geq 6$, while the inequalities in Theorem 2.3 show that this is the case for $k = 3, 4, 5$ as well.

3.2. Varying the characteristic. It is also interesting to look at Corollary 3.1, or to the more precise Theorem 2.3 when needed, from a different perspective, thinking of k as assigned and varying the prime p . The smallest value of k which is of interest here is $k = 5$. In fact, according to [Mat02, Corollary 3.4], no proper divisor of $p^3 - 1$ belongs to \mathcal{N}_p , with the only exception that $(3^3 - 1)/2 = 13 \in \mathcal{N}_3$. Moreover, when $k = 4$ and $p > 2$ the number $(p^4 - 1)/2$ is a multiple of $p^2 - 1$ and, hence, is a trivial element of \mathcal{N}_p . When $k = 5$, Theorem 2.3 implies that $(p^5 - 1)/2 \in \mathcal{N}_p$ for $p = 3, 5$, as mentioned above. (As reported in [Mat02, Example 4.1], direct calculations show that $(p^5 - 1)/2 \in \mathcal{N}_p$ for $p = 7, 11$ as well, but not for $p = 13$.) Similarly, Theorem 2.3 implies that $(p^7 - 1)/2 \in \mathcal{N}_p$ for $p = 3, 5, 7$.

In this respect we should note that, for a fixed prime k , there can only be finitely many primes p such that $p^k - 1$ has a proper divisor in \mathcal{N}_p . This follows from a result of H. Davenport [Dav37, Theorem 1]: given $k > 1$ (not necessarily prime), if the prime p is sufficiently large (depending only on k) and $\mathbb{F}_{p^k} = \mathbb{F}_p(\xi)$, then there exists $\lambda \in \mathbb{F}_p$ such that $\xi + \lambda$ is a primitive element of \mathbb{F}_{p^k} . Under our present assumption that k is prime, any element $\xi \in \mathbb{F}_{p^k}$ chosen as in Theorem 2.1 satisfies $\mathbb{F}_{p^k} = \mathbb{F}_p(\xi)$, and then Davenport's theorem implies that $p^k - 1$ divides n if p is sufficiently large.

3.3. Computer calculations. Since \mathcal{N}_p is closed with respect to taking multiples, the following definition is convenient: call *minimal* any number in \mathcal{N}_p which has no proper divisor in \mathcal{N}_p . (In the terminology of [HR83, Chapter V], the minimal elements of \mathcal{N}_p form the *primitive generating sequence* of \mathcal{N}_p .) A computer search has shown that the minimal elements of \mathcal{N}_2 below 200000 are

$$\begin{aligned} 3 &= 2^2 - 1, & 7 &= 2^3 - 1, & 31 &= 2^5 - 1, & 73 &= (2^9 - 1)/7, & 85 &= (2^8 - 1)/3, \\ 127 &= 2^7 - 1, & 2047 &= 2^{11} - 1, & 3133 &= (2^{24} - 1)/5355, & 4369 &= (2^{16} - 1)/15, \\ 8191 &= 2^{13} - 1, & 11275 &= (2^{20} - 1)/93, & 49981 &= (2^{30} - 1)/21483, \\ 60787 &= (2^{22} - 1)/69, & 76627 &= (2^{36} - 1)/896805, & 121369 &= (2^{39} - 1)/4529623, \\ 131071 &= 2^{17} - 1, & 140911 &= (2^{28} - 1)/1905, & 178481 &= (2^{23} - 1)/47. \end{aligned}$$

Of the nontrivial elements in this list, only 85 and 4369 are explained by Corollary 2.5. For other elements in the list, Corollary 2.5 (or Theorem 2.3) is only strong enough to show that certain of their multiples, still within the range considered, are nontrivial elements of \mathcal{N}_p . As an example, this is the case for $11275 \cdot 3 = (2^{20} - 1)/31$. Another fact which follows from inspection of the table, together with the observation that $2^{19} - 1$ is a prime, is that $2^{23} - 1$ is the smallest element of \mathcal{N}_2 , of the form $2^k - 1$ with k prime, which is not minimal.

We have carried out similar calculations for $p = 3$. They have shown that the minimal elements of \mathcal{N}_3 below 100000 are

$$\begin{aligned} 8 &= 3^2 - 1, & 13 &= (3^3 - 1)/2, & 121 &= (3^5 - 1)/2, \\ 1093 &= (3^7 - 1)/2, & 88573 &= (3^{11} - 1)/2, \end{aligned}$$

all of which are predicted by Theorem 2.3, as discussed above. The smallest prime k for which Theorem 2.3 produces a proper divisor of $3^k - 1$ in \mathcal{N}_3 different from $(3^k - 1)/2$ is 23, namely, we have $(3^{23} - 1)/47 \in \mathcal{N}_3$. Note that such a number would be far too large for a direct verification that it belongs to \mathcal{N}_3 based on the characterization given in Theorem 2.1. Because of the computational complexity of an exhaustive search we were not able to produce any element of \mathcal{N}_3 which is not predicted by Theorem 2.3.

For each prime p larger than 3 we know of essentially only one element of \mathcal{N}_p which is not within the range where Theorem 2.3 applies, namely, the number $(p^p - 1)/(p - 1)$ noted by Shalev in [Sha99, Example 2.6]. This is also the smallest element of \mathcal{N}_p which we know of for a generic prime $p > 3$. (The element $(p^k - 1)/2$ produced by Corollary 3.1 is larger than that.)

3.4. Density of \mathcal{N}_p . A referee has suggested to look at the density of \mathcal{N}_p . It is not clear whether \mathcal{N}_p possesses a *natural density* $\lim_{m \rightarrow \infty} |\{n \in \mathcal{N}_p \mid n \leq m\}|/m$. However, since \mathcal{N}_p is closed with respect to taking multiples, a result of Davenport and Erdős [HR83,

Chapter V, Theorem 12] guarantees that \mathcal{N}_p possesses a *logarithmic density*

$$\delta(\mathcal{N}_p) = \lim_{m \rightarrow \infty} \frac{1}{\log m} \sum_{n \in \mathcal{N}_p, n \leq m} \frac{1}{n},$$

and that $\delta(\mathcal{N}_p)$ coincides with the *lower asymptotic density*, $\liminf_{m \rightarrow \infty} |\{n \in \mathcal{N}_p \mid n \leq m\}|/m$.

It would be interesting to know how much $\delta(\mathcal{N}_p)$ exceeds $\delta(\mathcal{T}_p)$, where \mathcal{T}_p consists of the trivial elements of \mathcal{N}_p , that is, of all multiples of numbers of the form $p^k - 1$ for some $k \geq 2$. Since \mathcal{T}_p coincides with the set of multiples of numbers of the form $p^k - 1$ with k prime, and because $p^k - 1$ and $p^{k'} - 1$ have greatest common divisor $p - 1$ for different primes k and k' , one easily sees that \mathcal{T}_p possesses a natural density, whose value equals

$$\delta(\mathcal{T}_p) = \frac{1}{p-1} \left(1 - \prod_{k \text{ prime}} \left(1 - \frac{p-1}{p^k-1} \right) \right).$$

For example, when $p = 2$ one has $\delta(\mathcal{N}_2) \geq \delta(\mathcal{T}_2) \approx 0.451699$.

It is not clear how Theorem 2.2 can be efficiently used to improve this trivial lower bound for $\delta(\mathcal{N}_p)$. In the case of $p = 2$ we sketch how to obtain a small improvement by considering certain nontrivial elements of \mathcal{N}_2 exhibited in [Mat]. It was shown there that $(2^{st} - 1)/(2^s - 1)$ belongs to \mathcal{N}_2 , for $s \geq 1$ and $t \geq 3$. This is a consequence of Theorem 2.2 for $t \geq 4$, but not for $t = 3$, in which case the conclusion follows from a direct calculation given in [Mat, Proposition 2.2]. Note that, by taking $s = 1$, the numbers considered here include all numbers of the form $2^t - 1$, except 3. Denoting by \mathcal{S} the set of positive integers which are either multiples of 3 or of some number of the form $(2^{st} - 1)/(2^s - 1)$, with $s \geq 1$ and $t \geq 3$, we have $\mathcal{T}_2 \subseteq \mathcal{S} \subseteq \mathcal{N}_2$. According to [Mat, Proposition 3.4] and the following comments, \mathcal{S} equals the set of multiples of numbers in the set

$$\{3\} \cup \left\{ \frac{2^{2^{a+2}} - 1}{2^{2^a} - 1} \mid a \geq 1 \right\} \cup \left\{ \frac{2^{r^{b+1}} - 1}{2^{r^b} - 1} \mid r \text{ odd prime, } b \geq 0 \right\}.$$

Using the fact that the numbers of this set are mostly pairwise coprime, with some exceptions detailed in [Mat, Proposition 3.4], and performing some numerical calculations we have found that $\delta(\mathcal{N}_2) \geq \delta(\mathcal{S}) \approx 0.465673$. By adding to the set \mathcal{S} the multiples of the elements of \mathcal{N}_2 listed in Subsection 3.3 (which are the minimal elements of \mathcal{N}_2 not exceeding 200000) we can still improve the lower bound for $\delta(\mathcal{N}_2)$ a little bit and obtain that $\delta(\mathcal{N}_2) \geq 0.465926$.

3.5. Relative size of elements of \mathcal{N}_p . Our main result, especially in the slightly weaker but simpler form of Corollary 2.5, suggests that it may be interesting to introduce a relative measure of the size of a divisor n of $p^k - 1$. There are several good candidates for this quantity, all close to $\log_p(n)/k$ for n large, where k is taken as small as possible, hence $k = \text{ord}_n(p)$, the (multiplicative) order of p modulo n . For the present discussion we select the following. For an integer n prime to p , we define its *relative size* with respect to p as the quantity $\log(n)/\log(p^{\text{ord}_n(p)} - 1)$. With this definition, numbers of the form $p^k - 1$ have relative size 1. Now we discuss what we know about the relative size of elements of \mathcal{N}_p .

The sufficient condition for $n \in \mathcal{N}_p$ given in Corollary 2.5 can be roughly read as the relative size of n being slightly larger than $1 - 1/(2p)$. However, the distinguished element $(p^p - 1)/(p - 1)$ of \mathcal{N}_p has relative size close to $1 - 1/p$. When $p = 2$, Corollary 2.5 says

precisely that any odd number of relative size at least $3/4$ belongs to \mathcal{N}_2 . The element $(2^{3s} - 1)/(2^s - 1)$ of \mathcal{N}_2 has relative size close to $2/3$, for s large. Several of the minimal elements of \mathcal{N}_2 listed in Subsection 3.3 have even smaller relative size, the smallest, close to 0.433052, being attained by 121369.

Note that \mathcal{N}_p contains elements of arbitrarily small relative size, simply because it is closed with respect to taking multiples. A simple way to see that is as follows. For a prescribed element n of \mathcal{N}_p consider a prime r , different from p . Then nr belongs to \mathcal{N}_p and has relative size $\log(nr)/\log(p^{\text{ord}_{nr}(p)} - 1) \leq 2\log(nr)/(\text{ord}_r(p) \cdot \log p)$. By an appropriate choice of r the latter quantity can be made arbitrarily small, because the function $\text{ord}_r(p)/\log r$ of the prime r is unbounded, as is easy to see (in fact, much stronger statements hold, see [EM99]). This argument, however, does not answer the question of whether *minimal* elements of \mathcal{N}_p can have arbitrarily small relative size.

4. THE NUMBER OF SOLUTIONS OF A CERTAIN SYSTEM OF EQUATIONS

The following proof of Theorem 2.2 depends on Lemma 4.1, which we postpone for clarity.

Proof of Theorem 2.2. Let N be the number of solutions over \mathbb{F}_q of the system of equations

$$\begin{cases} y_1^d = x \\ y_2^d = x + 1 \\ \vdots \\ y_r^d = x + r - 1 \end{cases}$$

An element ξ of \mathbb{F}_q such that $\xi, \xi + 1, \dots, \xi + r - 1$ are d th powers in \mathbb{F}_q corresponds to d^r distinct solutions of the system if none of the $\xi, \xi + 1, \dots, \xi + r - 1$ equals zero, and to d^{r-1} solutions otherwise. Since altogether these account for all solutions of the system, we have $N = d^r M + d^{r-1} M_0$, and the desired inequality follows from Lemma 4.1. \square

Lemma 4.1. *Let d be a divisor of $q - 1$ and let $0 < r \leq p$. Then the number N of solutions over \mathbb{F}_q of the system of equations*

$$(4.1) \quad \begin{cases} y_1^d = x \\ y_2^d = x + 1 \\ \vdots \\ y_r^d = x + r - 1 \end{cases}$$

satisfies

$$|N + d^{r-1} - q - 1| \leq ((rd - r - d - 1)d^{r-1} + 2)\sqrt{q}.$$

Proof. Let χ be a multiplicative character of \mathbb{F}_q of (exact) order d . Then all characters of order dividing d are given by the powers χ^i , for $i = 0, \dots, d-1$. For each $j = 1, \dots, r$, and for any given $\xi \in \mathbb{F}_q$, the sum

$$\sum_{i=0}^{d-1} \chi^i(\xi + j - 1) = \sum_{i=0}^{d-1} \chi((\xi + j - 1)^i)$$

(reading 0^0 as 1 when it occurs as the argument of χ) equals the number of solutions of $y_j^d = \xi + j - 1$. Therefore, the product of all these quantities equals the number of

solutions of the system having $x = \xi$. Consequently, the total number of solutions of system (4.1) is given by

$$(4.2) \quad N = \sum_{i_1=0}^{d-1} \cdots \sum_{i_r=0}^{d-1} \sum_{\xi \in \mathbb{F}_q} \chi(\xi^{i_1}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r}).$$

It remains to evaluate or bound the character sum $\sum_{\xi \in \mathbb{F}_q} \chi(\xi^{i_1}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r})$, depending on the r -tuple (i_1, \dots, i_r) . The sum takes the value q for the r -tuple $(0, \dots, 0)$. This case aside, the polynomial $z^{i_1}(z+1)^{i_2} \cdots (z+i-1)^{i_r}$ is never a d th power in $\mathbb{F}_p[z]$. Therefore, Weil's bound for character sums [LN83, Theorem 5.41] applies and yields that

$$(4.3) \quad \left| \sum_{\xi \in \mathbb{F}_q} \chi(\xi^{i_1}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r}) \right| \leq (w(i_1, \dots, i_r) - 1)\sqrt{q},$$

where $w(i_1, \dots, i_r)$ is the number of distinct roots in \mathbb{F}_q of the polynomial $z^{i_1}(z+1)^{i_2} \cdots (z+i-1)^{i_r}$. Clearly, $w(i_1, \dots, i_r)$ equals the number of nonzero entries in the r -tuple (i_1, \dots, i_r) . Adding together all character sums corresponding to the r -tuples different from $(0, \dots, 0)$, and using the triangle inequality, we obtain that $|N - q|$ does not exceed \sqrt{q} times the integer obtained by subtracting from $(d^r - 1)(r - 1)$ the total number of zero entries appearing in the collection of nonzero r -tuples. The total number of those zeroes equals $rd^{r-1} - r$, because zero occurs as many times as any other integer $1, \dots, d - 1$ in the whole set of r -tuples including $(0, \dots, 0)$. We conclude that

$$(4.4) \quad |N - q| \leq ((dr - r - d)d^{r-1} + 1)\sqrt{q}.$$

This inequality is close to our goal, but can still be improved a little (see Remark 4.2). The number of r -tuples $(i_1, \dots, i_r) \neq (0, \dots, 0)$ such that $i_1 + \cdots + i_r \equiv 0 \pmod{d}$ is $d^{r-1} - 1$. Consider any one of them. Then at least one of the entries i_j is positive, say i_1 without loss of generality. Since $\chi(\xi^d) = 1$ for $\xi \in \mathbb{F}_q^*$ and $\chi(0) = 0$, we have

$$\begin{aligned} \sum_{\xi \in \mathbb{F}_q} \chi(\xi^{i_1}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r}) &= \sum_{\xi \in \mathbb{F}_q^*} \chi(\xi^{-i_2-i_3-\cdots-i_r}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r}) \\ &= \sum_{\xi \in \mathbb{F}_q^*} \chi((1+\xi^{-1})^{i_2} \cdots (1+(r-1)\xi^{-1})^{i_r}) \\ &= \sum_{\eta \in \mathbb{F}_q^*} \chi((1+\eta)^{i_2} \cdots (1+(r-1)\eta)^{i_r}) \\ &= -1 + \sum_{\eta \in \mathbb{F}_q} \chi((1+\eta)^{i_2} \cdots (1+(r-1)\eta)^{i_r}) \end{aligned}$$

The polynomial $(1+z)^{i_2} \cdots (1+(r-1)z)^{i_r}$, which provides the argument for χ in the last character sum, has exactly $w(i_1, \dots, i_r) - 1$ distinct roots, that is, one less than the polynomial corresponding to the original sum. Therefore, for the character sums under present consideration inequality (4.3) can be strengthened to

$$\left| 1 + \sum_{\xi \in \mathbb{F}_q} \chi(\xi^{i_1}(\xi+1)^{i_2} \cdots (\xi+r-1)^{i_r}) \right| \leq (w(i_1, \dots, i_r) - 2)\sqrt{q}.$$

It follows that the coefficient of \sqrt{q} in inequality (4.4) can be decreased by 1 for each of those $d^{r-1} - 1$ character sums considered here, provided we increase $N - q$ by a constant term 1 each time. The desired inequality now follows. \square

Remark 4.2. The estimate for M given in [LN83, Exercise (5.66)] (for a more general question, but that greater generality is inessential) is

$$\left| M - \frac{q}{d^r} \right| \leq \left(r - 1 - \frac{r}{d} + \frac{1}{d^r} \right) \sqrt{q} + \frac{r}{d},$$

and hence has the coefficient of \sqrt{q} about $1/d$ larger than the estimate given in Theorem 2.2. Since the values of d of present interest to us may be much smaller than \sqrt{q} (namely, roughly of the size of $q^{1/2p}$, see Corollary 2.5), this makes a significant difference (in Theorem 2.3). The larger coefficient of \sqrt{q} given in [LN83, Exercise (5.66)] results from being content with inequality (4.4) in the proof of Lemma 4.1 (and thus, essentially, disregarding the effect of points at infinity). For example, when $r = 2$ it yields the weaker bound $|N - q| \leq (d - 1)^2 \sqrt{q}$ rather than Weil's bound $|N - d - q - 1| \leq (d - 1)(d - 2) \sqrt{q}$ for the Fermat curve $y_2^d - y_1^d = 1$.

Remark 4.3. The inequality proved in Lemma 4.1 is exactly Weil's bound $|\bar{N} - q - 1| \leq 2g\sqrt{q}$ for the number \bar{N} of \mathbb{F}_q -rational projective points of the curve in the projective space \mathbb{P}^{r+1} given by the system (4.1) in affine coordinates. In fact, the only singularity of the curve represented by (4.1) occurs at its point at infinity, which has multiplicity d^{r-1} . An efficient way to compute the genus g is to consider the nonsingular curve in \mathbb{P}^r , which is birationally equivalent to (4.1) via a projection, given in affine coordinates by

$$\begin{cases} y_2^d = y_1^d + 1 \\ y_3^d = y_2^d + 1 \\ \vdots \\ y_r^d = y_{r-1}^d + 1 \end{cases}$$

Because this curve is (nonsingular and) a complete intersection of hypersurfaces, one can compute its genus by means of the Adjunction Formula and its iterates (see [Har77, V, Proposition 1.5]). For a complete intersection of s hypersurfaces of degrees d_1, \dots, d_s , the Adjunction Formula reads $2g - 2 = ((\sum_i d_i) - s - 2) \prod_i d_i$. Since the curve under consideration is a complete intersection of $r - 1$ hypersurfaces of degree d , the Adjunction Formula gives $2g - 2 = (rd - r - d - 1)d^{r-1}$, as desired. This argument gives a shorter but less elementary proof of Lemma 4.1 based on Weil's bound $|\bar{N} - q - 1| \leq 2g\sqrt{q}$.

REFERENCES

- [Dav37] H. Davenport, *On primitive roots in finite fields*, Quart. J. Math., Oxford Ser. **8** (1937), 308–312.
- [EM99] Pál Erdős and M. Ram Murty, *On the order of $a \pmod{p}$* , Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, pp. 87–97. MR MR1684594 (2000c:11152)
- [Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR MR0463157 (57 #3116)
- [HR83] Heini Halberstam and Klaus Friedrich Roth, *Sequences*, second ed., Springer-Verlag, New York, 1983. MR MR687978 (83m:10094)
- [Jac79] Nathan Jacobson, *Lie algebras*, Dover Publications Inc., New York, 1979, Republication of the 1962 original. MR MR559927 (80k:17001)
- [LN83] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983, With a foreword by P. M. Cohn. MR MR746963 (86c:11106)
- [Mat] S. Mattarei, *The orders of nonsingular derivations of modular Lie algebras of characteristic two*, Israel J. Math., in press, [arXiv:math.RA/0602668](https://arxiv.org/abs/math.RA/0602668).

- [Mat02] ———, *The orders of nonsingular derivations of modular Lie algebras*, Israel J. Math. **132** (2002), 265–275. MR MR1952625 (2003k:17024)
- [Sha99] Aner Shalev, *The orders of nonsingular derivations*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 254–260, Group theory. MR MR1717417 (2000k:17021)
- [Ste94] Serguei A. Stepanov, *Arithmetic of algebraic curves*, Monographs in Contemporary Mathematics, Consultants Bureau, New York, 1994, Translated from the Russian by Irene Aleksanova. MR MR1321599 (95j:11055)

E-mail address: `mattarei@science.unitn.it`

URL: `http://www-math.science.unitn.it/~mattarei/`

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI TRENTO, VIA SOMMARIVE 14, I-38050 POVO (TRENTO), ITALY